



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/858,011	05/14/2001	Ya-Huang Chen	1981002	2049
7590 11/03/2004			EXAMINER	
KEITH KLINE PRO-TECHTOR INTERNATIONAL SERVICES 20775 NORADA COURT SARATOGA, CA 95070-3018			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2133	

DATE MAILED: 11/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/858,011	Applicant(s) CHEN, YA-HUANG	
	Examiner Shewaye Gelagay	Art Unit 2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on May 14, 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 US C § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1, 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang United States Letters Patent Number 6,128,744 in view of Tello United States Letters Patent Number 6,463,537 and further in view of Mooney et al. United States Letters Patent Number 5,610,981.

As per claim 1:

Wang teach a method for preventing unauthorized access into a computer unit using a personal identification device and an input and output (I/O) control chip to control the activation of the computer unit, the steps comprising of:

(a) said personal identification device entering into a standby status; (Col. 2, line 64; uses a standby voltage when the computer system is turned off)

(b) inputting personal identification data into said personal identification device; (Col. 3; lines 6-7; read a user identification signal stored in the IC card)

(c) determining the validity of said personal identification data and returning to said step (a) if said personal identification data is invalid; (Col. 3; lines 7-8; generate a

verification signal when the computer identification signal matches the user identification signal)

(g) said I/O control chip activating said computer unit; (Col. 3; lines 8-10; the power control circuit is used to generate a start signal in response to the verification signal)

(h) said computer unit returns to normal operations; (Col. 3; line 10; the computer system is turned on)

(k) searching for new personal identification data and returning to step j) if not found; (Col. 3; lines 6-7; read a user identification signal stored in the IC card)

(l) determining the validity of said new personal identification data and returning to said step (h) if invalid; (Col. 3; lines 8-10; the power control circuit is used to generate a start signal in response to the verification signal)

(m) said personal identification device deactivating said suspend function and returning to step (h); and (Col. 3; lines 8-10; the power control circuit is used to generate a start signal in response to the verification signal)

(n) returning to normal operations for said computer unit. (Col. 3; line 10; the computer system is turned on)

Wang do not explicitly disclose (i) searching for said personal identification data in said personal identification device, and jumping to step (n) if said personal identification data are found; (j) said personal identification device activating a suspend function in said computer unit to stop all I/O operations, and informing said suspension to said authorized user through a personal identification data display.

Tello in analogous art, however, disclose

(i) searching for said personal identification data in said personal identification device, and jumping to step (n) if said personal identification data are found; (Col. 25, lines 30-31; the security engine microprocessor checks for the presence of a smart card in the attached smart card reader)

(j) said personal identification device activating a suspend function in said computer unit to stop all I/O operations, and informing said suspension to said authorized user through a personal identification data display; (Col. 25, lines 33-37; a request to the user to insert a smart card is given via a display and the start up procedure is terminated)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang to include (i) searching for said personal identification data in said personal identification device, and jumping to step (n) if said personal identification data are found; (j) said personal identification device activating a suspend function in said computer unit to stop all I/O operations, and informing said suspension to said authorized user through a personal identification data display. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Tello (Col. 4, lines 59-61) in order to provide a means for controlling access to a computer and sensitive data stored on its data storage devices during the operation of the computer.

Both references Wang and Tello teach all the subject matter described above. Neither of the references, however, teach explicitly (d) said personal identification device activating a control circuit, which allows said I/O control chip to activate a computer keyboard and displaying a notification message prompting an authorized user to enter a password; (e) said authorized user entering said password; (f) said I/O control chip determining validity of said password and returning to said step (e) if said password is invalid.

Mooney et al. in analogous art, however, disclose

(d) said personal identification device activating a control circuit, which allows said I/O control chip to activate a computer keyboard and displaying a notification message prompting an authorized user to enter a password; (Col. 6; lines 39-42; in order to gain access to the sensitive data information stored on hard drive, both card and card reader interface board must present proper identification information and the user must enter a series of predetermined answers to a series of predetermined questions)

(e) said authorized user entering said password; (Col. 6; lines 42-43; the user must enter a series of predetermined answers to a series of predetermined questions)

(f) said I/O control chip determining validity of said password and returning to said step (e) if said password is invalid; (Col. 14; lines 9-10; a retry counter is incremented each time an error is made in answering questions and is preprogrammed by the security administrator to terminate the verification program if number of erroneous responses exceeds the preprogrammed value)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang and Tello to include (d) said personal identification device activating a control circuit, which allows said I/O control chip to activate a computer keyboard and displaying a notification message prompting an authorized user to enter a password; (e) said authorized user entering said password; (f) said I/O control chip determining validity of said password and returning to said step (e) if said password is invalid. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Mooney et al. (Col. 6, line 36) in order to provide security by requiring distinct sources of authorization verification information.

As per claim 3:

Wang, Tello and Mooney et al. teach all the subject matter as described above. Wang further disclose a method wherein said personal identification device is a card reader. (Figure 1, item 12)

As per claim 4:

Wang, Tello and Mooney et al. teach all the subject matter as described above. Wang further disclose a method wherein said personal identification data are derived from an IC card. (Col. 2; lines 46-47; a smart card is provided to store a user identification signal)

3. Claims 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang United States Letters Patent Number 6,128,744 in view of Tello United States Letters Patent Number 6,463,537 in view of Mooney et al. United States Letters Patent

Number 5,610,981 and further in view of Yeom United States Letters Patent Number 5,911,080.

As per claim 2:

Wang, Tello and Mooney et al. teach all the subject matter as described above. Tello further disclose the security engine microprocessor checks for the presence of a smart card in the attached smart card reader (Col. 25, lines 30-31). Neither of the references, however, teach explicitly (o) searching for said personal identification data in a preset time period and jumping to step (q) if not found; (p) triggering an alarm through said personal identification device and returning to step (o); and (q) said identification device returning to a standby status.

Yeom in analogous art, however, teach

(o) searching for said personal identification data in a preset time period and jumping to step (q) if not found; (Col. 4; lines 35-37; the power control section reads the data of ID card inserted and repeats the above steps)

(p) triggering an alarm through said personal identification device and returning to step (o); and (Col. 4; lines 40-41; the power control section is turned off after a predetermined time interval)

(q) said identification device returning to a standby status. (Col. 4; lines 40-41; the power to the ID card reader is turned off after a predetermined time interval)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang, Tello and Mooney et al. to include (o) searching for said personal identification data in a preset

Art Unit: 2133

time period and jumping to step (q) if not found; (p) triggering an alarm through said personal identification device and returning to step (o); and (q) said identification device returning to a standby status. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to avoid unauthorized access while the computer is on by making sure the card is always in the card reader. This way, the computer system is protected not only when the computer is activated but also during its operation.

As per claim 6:

Wang, Tello and Mooney et al. teach all the subject matter as described above. Yeom further disclose a method wherein said preset time period is set for 10 seconds. (Col. 4; lines 63-44; the predetermined time interval can be set)

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang United States Letters Patent Number 6,128,744 in view of Tello United States Letters Patent Number 6,463,537 and in view of Mooney et al. United States Letters Patent Number 5,610,981 and further in view of Moseley United States Letters Patent Number 5,193,114.

As per claim 5:

Wang, Tello and Mooney et al. teach all the subject matter as described above. Neither of the references, however, teach explicitly a method wherein said personal identification data display is an LED.

Moseley in analogous art, however, teach a method wherein said personal identification data display is an LED. (Figure 2, item 28)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Wang, Tello and Mooney et al. to include a method wherein said personal identification data display is an LED. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to communicate with the smart card owner to input identification or any other information required. The LED is used to display messages on the personal identification device before the normal operations of the computer is started.

5. Claims 7, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang United States Letters Patent Number 6,128,744 in view of Tello United States Letters Patent Number 6,463,537 and further in view of Heinrich et al. United States Letters Patent Number 6,199,167

As per claim 7:

Wang teach an apparatus for a computer unit security system comprising:
personal identification data for use by a personal identification device for identifying an authorized user; and (Col. 3; lines 6-7; read a user identification signal stored in the IC card)

said personal identification-device having an I/O control circuit connected to said computer unit as to allow normal operations when said authorized user is identified, (Col. 3; lines 7-8; generate a verification signal when the computer identification signal matches the user identification signal)

Art Unit: 2133

Wang do not explicitly disclose suspending all operations of said computer unit when said personal identification data are removed prior to said computer unit being shut down, and preventing said computer unit from reactivation if said personal identification data is not revalidated.

Tello in analogous art, however teach suspending all operations of said computer unit when said personal identification data are removed prior to said computer unit being shut down, (Col. 25, lines 30-31; the security engine microprocessor checks for the presence of a smart card in the attached smart card reader) and preventing said computer unit from reactivation if said personal identification data is not revalidated. (Col. 25, lines 33-37; a request to the user to insert a smart card is given via a display and the start up procedure is terminated)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang to include suspending all operations of said computer unit when said personal identification data are removed prior to said computer unit being shut down, and preventing said computer unit from reactivation if said personal identification data is not revalidated. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Tello (Col. 4, lines 59-61) in order to provide a means for controlling access to a computer and sensitive data stored on its data storage devices during the operation of the computer.

Both references Wang and Tello teach all the subject matter described above. Neither of the references, however, teach explicitly wherein said computer unit comprises:

a processor; a North Bridge chip connected to said processor for controlling data flow between said processor and a PCI and allowing said processor to retrieve or save files from at least a memory and AGP; a South Bridge chip connected to said North Bridge chip and an I/O control chip and serving as a bridge between a USB interface and said I/O control device; said I/O control chip connected to said South Bridge chip for activating said computer unit after receiving a valid password inputted through a keyboard; and said keyboard connected to said personal identification device and said I/O control chip which activates said keyboard for inputting said valid password after said authorized user has been identified.

Heinrich et al. in analogous art, however, teach

a processor; (Figure 1, item 126)

a North Bridge chip connected to said processor for controlling data flow between said processor and a PCI and allowing said processor to retrieve or save files from at least a memory and AGP; (Figure 1, item 108)

a South Bridge chip connected to said North Bridge chip and an I/O control chip and serving as a bridge between a USB interface and said I/O control device; said I/O control chip connected to said South Bridge chip for activating said computer unit after receiving a valid password inputted through a keyboard; and (Figure 1, item 112)

Art Unit: 2133

said keyboard connected to said personal identification device and said I/O control chip which activates said keyboard for inputting said valid password after said authorized user has been identified. (Figure 1; Col. 3, line 33; the user enters the password at the keyboard)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang and Tello to include an apparatus wherein a processor; a North Bridge chip connected to said processor for controlling data flow between said processor and a PCI and allowing said processor to retrieve or save files from at least a memory and AGP; a South Bridge chip connected to said North Bridge chip and an I/O control chip and serving as a bridge between a USB interface and said I/O control device; said I/O control chip connected to said South Bridge chip for activating said computer unit after receiving a valid password inputted through a keyboard; and said keyboard connected to said personal identification device and said I/O control chip which activates said keyboard for inputting said valid password after said authorized user has been identified. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Heinrich et al. (Col. 2, line 51) in order to allow the password to be checked in a more secure environment before any operation on the system side is enabled.

As per claim 11:

Art Unit: 2133

Wang, Tello and Heinrich et al. teach all the subject matter as described above.

Wang further disclose an apparatus wherein said personal identification device is a card reader. (Figure 1, item 12)

As per claim 12:

Wang, Tello and Heinrich et al. teach all the subject matter as described above.

Wang further disclose an apparatus wherein said personal identification data are derived from an IC card. (Col. 2; lines 46-47; a smart card is provided to store a user identification signal)

6. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang United States Letters Patent Number 6,128,744 in view of Tello United States Letters Patent Number 6,463,537 and in view of Heinrich et al. United States Letters Patent Number 6,199,167 and further in view of Moseley United States Letters Patent Number 5,193,114.

As per claim 8:

Wang, Tello and Heinrich et al. teach all the subject matter as described above.

Neither of the references, however, teach explicitly an apparatus wherein said personal identification data display is an LED.

Moseley in analogous art, however, teach an apparatus wherein said personal identification device includes an LED. (Figure 2, item 28)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang, Tello and Heinrich et al. to include an apparatus wherein said personal identification data display

is an LED. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to communicate with the smart card owner to input identification or any other information required. The LED is used to display messages on the personal identification device before the normal operations of the computer is started.

As per claim 9:

Wang, Tello and Heinrich et al. teach all the subject matter as described above. Neither of the references, however, teach explicitly an apparatus wherein said personal identification device includes a timer for reminding said authorized user regarding the non-removal of said personal identification data within a preset time period after said computer unit has been deactivated.

Moseley in analogous art, however, teach an apparatus wherein said personal identification device includes a timer for reminding said authorized user regarding the non-removal of said personal identification data within a preset time period after said computer unit has been deactivated. (Col. 5; lines 17-18; all readers "beep" after the transaction to remind the owner to take his card)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang, Tello and Heinrich et al. to include an apparatus wherein said personal identification device includes a timer for reminding said authorized user regarding the non-removal of said personal identification data within a preset time period after said computer unit has been deactivated. This modification would have been obvious because a person having

Art Unit: 2133

ordinary skill in the art would have been motivated to do so, in order to avoid access of the computer system by an unauthorized user. A beep will remind the smart card owner to remove the card right after the computer system is shut down.

7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang United States Letters Patent Number 6,128,744 in view of Tello United States Letters Patent Number 6,463,537 and in view of Heinrich et al. United States Letters Patent Number 6,199,167 and further in view of Yeom United States Letters Patent Number 5,911,080.

As per claim 10:

Wang, Tello and Heinrich et al. teach all the subject matter as described above. Neither of the references, however, teach explicitly an apparatus wherein said preset time period is set for 10 seconds.

Yeom in analogous art, however, teach an apparatus wherein said preset time period is set for 10 seconds. (Col. 4; lines 63-44; the predetermined time interval can be set)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wang, Tello and Heinrich et al. to include an apparatus wherein said preset time period is set for 10 seconds. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to avoid unauthorized access while the computer is on by checking periodically if the card is in the card

Art Unit: 2133

reader. This way, the computer system is protected not only when the computer is activated but also during its operation.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Flyntz U.S. 6,351,817

This reference pertains to multi-level secure computer with token-based access control.

b. Shinn U.S. 6,655,858

This reference pertains to a system and method of biometric smart card user authentication.

c. Craig et al. U.S. 6,260,111

This reference pertains to system and method for network power management incorporating user identity and preferences via power managed smart card.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2133

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

10/29/04

Shewaye Gelagay
Examiner
Art Unit 2133



GUY J. LAMARRE
PRIMARY EXAMINER